eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **Hashcat:**
  - ✓ Conhecendo o Hascat
  - ✓ Entendendo oclHashcat-plus
  - ✓ Características
  - ✓ Tipos de Hashes
  - ✓ Hashes específicas
  - ✓ Modos de ataques
  - ✓ Performance
  - ✓ Modos de uso

HASH CAT

HASHCAT

Advanced Password Recovery

Conhecendo Hashcat

O **hashcat** é uma ferramenta conhecida para uma boa parte dos profissionais que lidam com *pentest*.

Para quem ingressou recentemente no ramo de segurança e ainda não conhece suas funcionalidades, vamos falar um pouco sobre elas nesta aula.

Este utilitário tem a capacidade de quebrar e recuperar senhas, da mesma forma que o conhecido John the Ripper faz.

Entretanto, ao fazer uma comparação entre o **hashcat** e o **John the Ripper (JTR)**, existe diferenças em relação ao primeiro utilitário. O **hashcat** (em muitos algoritmos), apresenta maior rapidez, inclusive nas últimas competições relacionadas à quebras de senhas promovidas durante a Conferência Hacker DefCon, haviam grupos de competidores que utilizavam o **hashcat** (Oclhashcat) como ferramenta chave, incluindo o grupo que venceu a competição.

Além disso, a ferramenta possui uma característica única, devido a sua grande intuitividade na apresentação de uma interface gráfica.

Conhecendo Hashcat

Dentre as características que o **hashcat** apresenta, podemos dizer que ele é:

- Multi-Threaded;
- Free;
- Multi-Hash;
- Mais de 24 milhões de hashes;
- Multi-OS (incluindo sistemas Linux e Windows);
- Multi-Algorítimo, incluindo MD4, MD5, SHA1, DCC, NTLM, MySQL

Os modos de ataques também podem ser otimizados utilizando "rules", com exceção de ataques "Brute-force" e "Permutation".

O sistema de "Rules" é bastante rápido, apresentando compatibilidade com com JTR e PasswordsPro. Há também a possibilidade de limitar uma sessão de quebra, ou começar do ponto onde parou.

O hashcat pode, de forma automática, gerar "rules" randômicas.

Conhecendo Hashcat

A ferramenta também apresenta a possibilidade de selecionar várias *wordlists* ou até diversos diretórios com várias *wordlists*.

Vale ressaltar que a quantidade de "threads" pode ser configurada.

Além disso, mais de 30 algoritmos foram implementados, enfatizando questões relacionadas à performance do utilitário.

Fonte: Underlinux

Entendendo oclHashcat-plus

eSecurity

oclHashcat-plus é o primeiro e único mecanismo de regras do mundo baseado em GPGPU, além de ser o mais rápido cracker de hash de criptografias md5crypt, phpass, mscash2 e WPA / WPA2.

Dentre as características desse utilitário, estão incluídos uma plataforma Multi-GPU (de até 16 GPUs), um sistema Multi-Hash (suportando até 24 milhões de *hashes*), além de ser Multi-OS (oferecendo suporte para Linux e nativos binários do Windows) e possibilitando que o usuário interaja a partir de uma baixa utilização de recursos, podendo assistir seus filmes preferidos ou jogar, enquanto executa técnicas de *cracking*.

Características do Hashcat

O HashCat possui as seguintes características:

- Multi-Thread
- Multi-Hash (mais de 24 milhões de hashes)
- Multi-OS (Linux, Windows e OSX)
- Multi-Algo (MD4, MD5, SHA1, DCC, NTLM, MySQL, …)
- Rules compatíveis com JTR e PasswordsPro
- É possível continuar uma sessão de onde parou
- Pode trabalhar em ambiente distribuído
- Pode utilizar múltiplas wordlists inclusive especificando mais de um diretório contendo wordlists
- Número de threads pode ser configurado

Tipos de Hashes

O hashcat possui uma tabela de códigos para cada hash a ser quebrada. Caso você tenha a intenção de quebrar a Hash do Fórum vBulletin inferior ao 3.8.5, usará a opção –m5, se for apenas md5, use a opção –m0, e assim sucessivamente.

0 = MD5
1 = md5($pass.$salt)
2 = md5($salt.$pass)
3 = md5(md5($pass))
4 = md5(md5(md5($pass)))
5 = vBulletin < v3.8.5
6 = md5(md5($salt).$pass)
7 = md5($salt.md5($pass))
8 = md5($salt.$pass.$salt)
9 = md5(md5($salt).md5($pass))
10 = md5(md5($pass).md5($salt))
11 = md5($salt.md5($salt.$pass))
12 = md5($salt.md5($pass.$salt))
15 = vBulletin > v3.8.5

40 = md5($salt.unicode($pass))
50 = HMAC-MD5 (key = $pass)
60 = HMAC-MD5 (key = $salt)
100 = SHA1
110 = sha1($pass.$salt)
120 = sha1($salt.$pass)
130 = sha1(unicode($pass).$salt)
140 = sha1($salt.unicode($pass))
150 = HMAC-SHA1 (key = $pass)
160 = HMAC-SHA1 (key = $salt)
200 = MySQL
300 = MySQL4.1/MySQL5
400 = phpass, MD5(Wordpress), MD5(phpBB3)

Tipos de Hashes

500 = md5crypt, MD5(Unix), FreeBSD MD5, Cisco-IOS MD5
800 = SHA-1(Django)
900 = MD4
1000 = NTLM
1100 = Domain Cached Credentials, mscash
1400 = SHA256
1410 = sha256($pass.$salt)
1420 = sha256($salt.$pass)
1430 = sha256(unicode($pass).$salt)
1440 = sha256($salt.unicode($pass))
1450 = HMAC-SHA256 (key = $pass)
1460 = HMAC-SHA256 (key = $salt)
1600 = md5apr1, MD5(APR), Apache MD5
1700 = SHA512
1710 = sha512($pass.$salt)

1720 = sha512($salt.$pass)
1730 = sha512(unicode($pass).$salt)
1740 = sha512($salt.unicode($pass))
1750 = HMAC-SHA512 (key = $pass)
1760 = HMAC-SHA512 (key = $salt)
1800 = SHA-512(Unix)
2400 = Cisco-PIX MD5
2500 = WPA/WPA2
2600 = Double MD5
3200 = bcrypt, Blowfish(OpenBSD)
3300 = MD5(Sun)
3500 = md5(md5(md5($pass)))
3610 = md5(md5($salt).$pass)
3710 = md5($salt.md5($pass))
3720 = md5($pass.md5($salt))
3810 = md5($salt.$pass.$salt)
3910 = md5(md5($pass).md5($salt))
4010 = md5($salt.md5($salt.$pass))

Tipos de Hashes

www.eSecurity.com.br

4110 = md5($salt.md5($pass.$salt))
4210 = md5($username.0.$pass)
4300 = md5(strtoupper(md5($pass)))
4400 = md5(sha1($pass))
4500 = sha1(sha1($pass))
4600 = sha1(sha1(sha1($pass)))
4700 = sha1(md5($pass))
4800 = MD5(Chap)
5000 = SHA-3(Keccak)
5100 = Half MD5
5200 = Password Safe SHA-256
5300 = IKE-PSK MD5
5400 = IKE-PSK SHA1
5500 = NetNTLMv1-VANILLA / NetNTLMv1-ESS
5600 = NetNTLMv2
5700 = Cisco-IOS SHA256
5800 = Samsung Android Password/PIN

6300 = AIX {smd5}
6400 = AIX {ssha256}
6500 = AIX {ssha512}
6700 = AIX {ssha1}
6900 = GOST, GOST R 34.11-94
7000 = Fortigate (FortiOS)
7100 = OS X v10.8
7200 = GRUB 2
7300 = IPMI2 RAKP HMAC-SHA1
7400 = sha256crypt, SHA256(Unix)
9999 = Plaintext

Hashes específicas

O hashcat também faz a quebra de hashes específicas, são elas:

11 = Joomla
21 = osCommerce, xt:Commerce
101 = nsldap, SHA-1(Base64), Netscape LDAP SHA
111 = nsldaps, SSHA-1(Base64), Netscape LDAP SSHA
112 = Oracle 11g
121 = SMF > v1.1
122 = OS X v10.4, v10.5, v10.6
123 = EPi
131 = MSSQL(2000)
132 = MSSQL(2005)
141 = EPiServer 6.x < v4
1441 = EPiServer 6.x > v4

1711 = SSHA-512(Base64), LDAP {SSHA512}
1722 = OS X v10.7
1731 = MSSQL(2012)
2611 = vBulletin < v3.8.5
2711 = vBulletin > v3.8.5
2811 = IPB2+, MyBB1.2+
3721 = WebEdition CMS
7600 = Redmine Project Management Web App

Modos de ataques

Existem diferentes modos de se trabalhar com hashcat, segue abaixo:

- **Combination** – Você pode usar mais do que um dicionário para fazer a quebra. Se você possui 1 dicionário com 50 palavras e no outro 100, então ele irá mesclar esses 2 dicionários, criando então uma lista com 50 * 100 = 5000 palavras.

- **Table-Lookup** – Este modo de ataque também é baseado em dicionários, porém, você pode adicionar caracteres a serem substituídos em seus dicionários, por exemplo: a=A ou a=@ ou e=3 ficando em um dicionário 3s3curity.

- **Toggle-case** – Este método utiliza todas as letras maiúsculas e minúsculas de um dicionário. Por exemplo, vamos usar a palavra test. Neste caso ele irá tentar as seguintes combinações: Test, tEst, teSt e tesT.

- **Permutation** - Esta técnica não funciona muito bem, porém, caso um dia precise, estará ai para usa-la. Com este modo, você inverte caracteres de posição, por exemplo, usaremos a palavra pass123.
  pass123, pass321, 1pass23, 3pass21, 32pass1, 321pass, ...

Modos de ataques

- **Brute Force** – Ataque baseado em máscara, você define as regras de ataques e ele executa de acordo com a mascara que você selecionou. Ex: admin123 onde você queira que cada número seja entre 0 e 9.

- **Straight** – Opção básica e simples. Você seta uma wordlist e a hash a ser quebrada.

Performance

Performance

- PC1: Windows 7, 64 bit · Catalyst 14.9 · 1x AMD hd7970 · 1000mhz core clock · oclHashcat v1.31
- PC2: Ubuntu 14.04, 32 bit · ForceWare 340.24 · 1x NVidia gtx580 · stock core clock · oclHashcat v1.31
- PC3: Windows 7, 64 bit · ForceWare 344.75 · 1x NVidia gtx750Ti · stock core clock · oclHashcat v1.31
- PC4: Ubuntu 14.04, 64 bit · Catalyst 14.9 · 8x AMD R9 290X · stock core clock · oclHashcat v1.31

Hash Type	PC1	PC2	PC3	PC4
MD5	8511 Mh/s	2807 Mh/s	3115 Mh/s	93720 Mh/s
SHA1	2722 Mh/s	868 Mh/s	1103 Mh/s	29976 Mh/s
SHA256	1120 Mh/s	355 Mh/s	406 Mh/s	12312 Mh/s
SHA512	416 Mh/s	104 Mh/s	92 Mh/s	4576 Mh/s
SHA-3(Keccak)	179 Mh/s	93 Mh/s	93 Mh/s	1872 Mh/s
RipeMD160	1802 Mh/s	623 Mh/s	682 Mh/s	15552 Mh/s
Whirlpool	65800 kh/s	94792 kh/s	56104 kh/s	1007000 kh/s
LM	1374 Mh/s	447 Mh/s	428 Mh/s	13008 Mh/s
NTLM	16701 Mh/s	4256 Mh/s	5577 Mh/s	183528 Mh/s
NetNTLMv1	9066 Mh/s	2333 Mh/s	1357 Mh/s	71264 Mh/s
NetNTLMv2	591 Mh/s	206 Mh/s	133 Mh/s	4688 Mh/s
WPA/WPA2	141 kh/s	48 kh/s	52 kh/s	1149 kh/s

For example, PC4 can do 183528 Mh/s against NTLM, that is 183528000000 tries per second.

Modos de uso

Existem muitas maneiras de se usar o Hashcat, iremos exemplificar algumas maneiras simples de quebra de senhas e ao decorrer do curso, iremos aperfeiçoando nosso método de ataque.

Acesso ao Help:

hashcat –h

Quebrando hashes de forma simples (Straight):

hashcat hashes.txt word1.txt

Quebrando hashes de forma combinada (Combination):

hashcat --attack-mode 1 hashes.txt /tmp/word1.txt /tmp/word2.txt

Se você setar apenas o caminho das wordlists, ele irá utilizar todas as wls da pasta

Quebrando hashes de forma combinada, porém, setando 10 threads e arquivos de regras:

hashcat --attack-mode 1 --rules-file combinator.rule --threads 10 hashes.txt word1.txt word2.txt

Modos de uso

Depois de quebrar a Hash, você pode solicitar ao hashcat para remover os hashes encontrados para facilitar as quebras futuras:

hashcat --attack-mode 1 --remove hashes.txt word1.txt word2.txt

Setando a hash a ser quebrada (ex: SHA1):

hashcat --attack-mode 1 --hash-mode 100 --remove hashes.txt word1.txt word2.txt

Utilizando o modo Toggle e setando alternância no mínimo de caracter 1 com no máximo 7:

hashcat --attack-mode 2 --toggle-min 1 --toggle-max 7 hashes.txt word.txt word2.txt

Utilizando o modo Permutation, e setando alternância no mínimo de 1 e com o máximo de 7 caracteres

hashcat --attack-mode 4 --perm-min 1 --perm-max 7 hashes.txt word.txt word2.txt

Utilizando o modo Brute Force:

hashcat --attack-mode 3 hashes.txt

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker